ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 10, October 2018

Encryption Based Lossless and Reversible Data Hiding Survey

Amol Narkhede [1], Prof.Dinesh Patil [2]

P.G. Student, Department of Computer Science Engineering, SSGBCOE&T, Bhusawal, Maharashtra, India[1]

Associate Professor, Department of Computer Science Engineering, SSGBCOE&T, Bhusawal, Maharashtra, India[2]

ABSTRACT: Image processing is used to improve the quality of image. Now days, more focus is on reversible data hiding (RDH) in encrypted images, so it maintains the excellent property that the original cover image can be easily recovered without any loss after embedded data. All previous techniques embed data by reversibly vacating room from the encrypted images, which may be leads to some errors on data extraction and image restoration. In this paper, we propose a method by reserving room before encryption with a RDH algorithm and LSB algorithm, and thus it is easy for the user to reversibly embed data in the encrypted image. The proposed system is reversible, that is, data extraction and image recovery is without any loss. A reversible data hiding algorithm and LSB algorithm, which can recover the original image without any loss from marked image after the hidden data have been extracted. Experiments show that this RDH method can embed more than 10times as large payloads for the same image quality as the previous methods, such as for PSNR dB.

KEYWORDS: Reversible Data Hiding, Reserving Room, Vacating Room, Blowfish Algorithm Least Significant Bit Algorithm, Image/Data Embedding, Encryption/Decryption, Hide Key/Embed Key

I. INTRODUCTION

We say a data hiding strategy is reversible if the first cover substance can be impeccably recouped from the spread form containing implanted information despite the fact that a slight twisting has been presented in information inserting technique. Various components, for example, distinction extension, histogram shift and lossless pressure, have been utilized to build up the reversible information concealing procedures .so proposed methodology a combined data hiding schemes for cipher text images encrypted by public key cryptosystems with probabilistic and homomorphic properties. In the lossless scheme, the cipher text pixels are replaced with new values to embed the additional information into several LSB-planes of cipher text pixels by using 4LSB. Then, the embedded data can be directly extracted from the encrypted domain by using blowfish algorithm and the data embedding process does not affect the decryption of original plaintext image file. In the reversible procedure, a pre-handling is utilized to compress the image histogram before image encryption, so that the alteration on encoded image for information embedding does not create any pixel oversaturation in plaintext space. In spite of the fact that a little twisting is presented, the embedded information can be extracted and the first image record can be recover from the straightforwardly decrypted image. Because of the similarity between the lossless and reversible system, the information embedding forms in the two behaviour can be at the same time performed in a encrypted image. With the consolidated new system, a receiver might extricate a piece of embedded data before decoding, and extract other piece of embedded data of the record and recover the first plaintext image after decryption.

II. BRIEF DESCRIPTION

Encryption and information hiding are two viable methods for information security. While the encryption procedures change over plaintext content into mixed up cipher text, the information concealing strategies insert extra information into spread media by presenting slight alterations. In some mutilation unsuitable situations, information concealing may

DOI: 10.15680/IJIRCCE.2018. 0610006

be performed with a lossless or reversible way. In spite of the fact that the expressions "lossless" and "reversible" have a same which means in an arrangement of past references, we would recognize them in this work.

We say that information hiding technique is lossless if the display of cover signal containing installed information is same as that of unique cover despite the fact that the spread information have been adjusted for information inserting. For instance, the pixels with the most utilized shading as a part of a palette picture are doled out to some unused shading lists for conveying the extra information, and these files are diverted to the most utilized shading. Thusly, despite the fact that the files of these pixels are modified, the genuine shades of the pixels are kept unaltered. Then again, we say an information concealing system is reversible if the first cover substance can be consummately recouped from the spread rendition containing installed information despite the fact that a slight bending has been presented in information implanting strategy. Various instruments, for example, distinction extension, histogram shift and lossless pressure, have been utilized to build up the reversible information concealing systems for computerized pictures. As of late, a few decent forecast methodologies and ideal move likelihood under payload-mutilation measure have been acquainted with enhance the execution of reversible information covering up.

III. LITERATURE REVIEW

[1] data embedding over images has drawn tremendous interest, using either lossy or lossless techniques. Although lossy techniques can allow large hiding capacity, host image cannot be recovered with high fidelity. Some applications require exact recovery of the host image, i.e. in medicine patient data can be embedded without affecting the medical image. In general lossless data hiding techniques suffer from limited capacity as the host image should be kept intact. In this paper a lossless embedding technique is proposed. In this technique image histograms are analyzed to identify the embedding capacity of different image types. Histogram maxima and minima are used in embedding capacity estimation. The proposed technique gives hiding capacity that can reach up to 50% of the host image size for images with large homochromatic regions (cartoons-like). [2] stated Current difference-expansion (DE) embedding techniques perform one layer embedding in a difference image. They do not turn to the next difference image for another layer embedding unless the current difference image has no expandable differences left. The obvious disadvantage of these techniques is that image quality may have been severely degraded even before the later layer embedding begins because the previous layer embedding has used up all expandable differences, including those with large magnitude. Based on integer Haar wavelet transform, we propose a new DE embedding algorithm, which utilizes the horizontal as well as vertical difference images for data hiding. We introduce a dynamical expandable difference search and selection mechanism. This mechanism gives even chances to small differences in two difference images and effectively avoids the situation that the largest differences in the first difference image are used up while there is almost no chance to embed in small differences of the second difference image.[3] stated digital watermarking, often referred to as data hiding, has recently been proposed as a promising technique for information assurance. Owing to data hiding, however, some permanent distortion may occur and hence the original cover medium may not be able to be reversed exactly even after the hidden data have been extracted out. Following the classification of data compression algorithms, this type of data hiding algorithms can be referred to as lossy data hiding. It can be shown that most of the data hiding algorithms reported in the literature are lossy. Here, let us examine three major classes of data hiding algorithm. With the most popularly utilized spread-spectrum water- marking techniques, either in DCT domain or block 8x8 DCT domain round- off error and/or truncation error may take place during data embedding. As a result, there is no way to reverse the stago-media back to the original without distortion.[4] stated a novel lossless (reversible) data-embedding technique, which enables the exact recovery of the original host signal upon extraction of the embedded information. A generalization of the well-known least significant bit (LSB) modification is proposed as the data-embedding method, which introduces additional operating points on the capacity-distortion curve. Lossless recovery of the original is achieved by compressing portions of the signal that are susceptible to embedding distortion and transmitting these compressed descriptions as a part of the embedded payload. A prediction-based conditional entropy coder which utilizes unaltered portions of the host signal as side-information improves the compression efficiency and, thus, the lossless data-embedding capacity. [5] Stated Prediction-error expansion (PEE) - based reversible data hiding schemes consist of two steps. First, a sharp prediction-error (PE) histogram is generated by utilizing pixel prediction strategies. Second, secret messages are reversibly embedded into the prediction-errors through expanding and shifting the PE

histogram. Previous PEE methods treat the two steps independently while they either focus on pixel prediction to obtain a sharp PE histogram, or aim at histogram modification to enhance the embedding performance for a given PE histogram. This paper propose a pixel prediction method based on the minimum rate criterion for reversible data hiding, which establishes the consistency between the two steps in essence. And correspondingly, a novel optimized histograms modification scheme is presented to approximate the optimal embedding performance on the generated PE sequence. Experiments demonstrate that the proposed method outperforms the previous state-of-art counterparts significantly in terms of both the prediction accuracy and the final embedding performance.

IV. PROPOSED MODEL

A) Lossless Data System Consist of three parties:

- An image provider.
- A data hider.
- A receiver.

The role of image provider is to encrypt each pixel of the original plaintext image using the public key of the receiver. The data hider is unaware with the actual image. Data hider can edit the cipher text pixel values to embed some additional data into the encrypted image by multi-layer wet paper coding .There lies one condition that the decrypted values of new and original cipher-text pixel values must be unique. The receiver have the encrypted image containing the additional data, a receiver knowing the data hiding key may extract the embedded data, while a receiver with the private key of the cryptosystem may perform decryption to retrieve the original plaintext image. The embedded data can be extracted in the encrypted domain, and cannot be extracted after decryption. That means the data embedding does not affect the decryption of the plaintext image.

B) Reversible Data Hiding Scheme

To shrink the image histogram some preprocessing is employed in reversible scheme. Then each pixel is encrypted with additive homomorphic cryptosystem by the image provider. When data hider have the encrypted image, he modifies the cipher text pixel values to embed a bit-sequence generated from the additional data and error-correction codes. Due to the homomorphic property, the modification in encrypted domain will result in slight increase/decrease on plaintext pixel values. The advantage of histogram shrink before encryption is that the data embedding operation does not cause any overflow/underflow in the directly decrypted image[1].

C) Combined Data Hiding Scheme

A lossless and a reversible data hiding schemes for public-key-encrypted images are proposed. In both of the two schemes, the data embedding operations are performed in encrypted domain.

On the other hand, the data extraction procedures of the two schemes are very different. With the lossless scheme, data embedding does not affect the plaintext content and data extraction is also performed in encrypted domain.

With the reversible scheme, there is slight distortion in directly decrypted image caused by data embedding, and data extraction and image recovery must be performed in plaintext domain. That implies, on receiver side, the additional data embedded by the lossless scheme cannot be extracted after decryption, while the additional data embedded by the reversible scheme cannot extracted before decryption. In this section, we combine the lossless and reversible schemes to construct a new scheme, in which data extraction in either of the two domains is feasible

V. CONCLUSION

A survey on various reversible data hiding techniques is performed. Reversible data hiding schemes for encrypted image with a low computation complexity is analysed, which consists of image encryption, data hiding and data extraction/ image recovery phases. The original images are encrypted by an encryption strategy. So a study about an encryption strategy is performed. Although a data hider does not know the original content, he can embed the secret data into the encrypted image by modifying a part of encrypted data. So methods for data embedding are also noticed.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 10, October 2018

REFERENCES

1. N. A. Saleh, H. N. Boghdad, S. I. Shaheen, A. M. Darwish, "High Capacity Lossless Data Embedding Technique for Palette Images Based on Histogram Analysis," Digital Signal Processing, 20, pp. 1629−1636, 2010.
2. J. Tian, "Reversible Data Embedding Using a Difference Expansion," IEEE Trans. on Circuits and Systems for Video Technology, 13(8), pp. 890−896, 2003.
3. Z. Ni, Y.-Q. Shi, N. Ansari, and W. Su, "Reversible Data Hiding," IEEE Trans. on Circuits and Systems for Video Technology, 16(3), pp. 354−362, 2006.
4. M. U. Celik, G. Sharma, A. M. Tekalp, and E. Saber, "Lossless Generalized-LSB Data Embedding," IEEE Trans. on Image Processing, 14(2), pp. 253–266, 2005
5. X. Hu, W. Zhang, X. Li, and N. Yu, "Minimum Rate Prediction and Optimized Histograms Modification for Reversible Data Hiding," IEEE Trans. on Information Forensics and Security, 10(3), pp. 653-664, 2015.
6. S. Lian, Z. Liu, Z. Ren, and H. Wang, "Commutative Encryption and Watermarking in Video Compression," IEEE Trans. on Circuits and Systems for Video Technology, 17(6), pp. 774−778, 2007.
7. M. Cancellaro, F. Battisti, M. Carli, G. Boato, F. G. B. Natale, and A. Neri, "A Commutative Digital Image Watermarking and Encryption Method in the Tree Structured Haar Transform Domain," Signal Processing: Image Communication, 26(1), pp. 1−12, 2011.
8. W. Puech, M. Chaumont, and O. Strauss, "A Reversible Data Hiding Method for Encrypted Images," Security, Forensics, Steganography, and Watermarking of Multimedia Contents X, Proc. SPIE, 6819, 2008.
9. M. S. A. Karim, and K. Wong, "Universal Data Embedding in Encrypted Domain," Signal Processing, 94, pp. 174-182, 2014.
10. M. U. Celik, G. Sharma, A. M. Tekalp, and E. Saber, "Lossless Generalized-LSB Data Embedding," IEEE Trans. on Image Processing, 14(2), pp. 253–266, 2005
11. X. Hu, W. Zhang, X. Li, and N. Yu, "Minimum Rate Prediction and Optimized Histograms Modification for Reversible Data Hiding," IEEE Trans. on Information Forensics and Security, 10(3), pp. 653-664, 2015
12. M. S. A. Karim, and K. Wong, "Universal Data Embedding in Encrypted Domain," Signal Processing, 94, pp. 174-182, 2014.
13. P. Paillier, "Public-Key Cryptosystems Based on Composite Degree Residuosity Classes," Proceeding of the Advances Cryptology, EUROCRYPT'99, LNCS, 1592, pp. 223-238, 1999.